(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－518724
（P2001－518724A）
(43)公表日　平成13年10月16日(2001.10.16)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	12/66		Ｇ０６Ｆ	13/00	３５１Ｚ　５Ｂ０８９
Ｇ０６Ｆ	13/00	３５１			６１０Ｓ　５Ｊ１０４
		６１０			Ｂ　５Ｋ０３０
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	11/20	６４１
	12/54			9/00	
				11/20	１０１Ｂ

審査請求　未請求　予備審査請求　有　（全 40 頁）　最終頁に続く

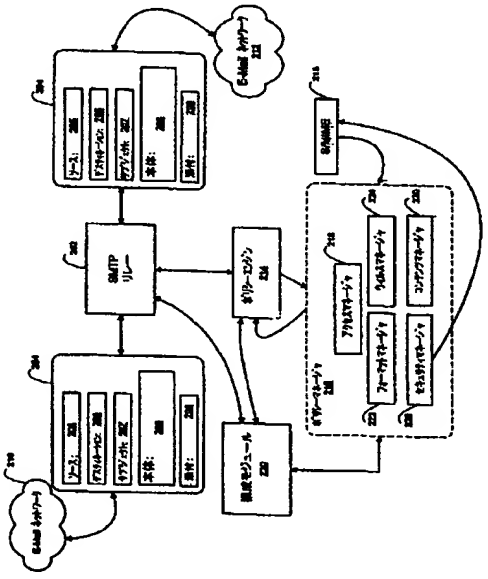
(21)出願番号　特願2000－504677(P2000－504677)
(86)(22)出願日　平成10年７月23日(1998.7.23)
(85)翻訳文提出日　平成12年１月24日(2000.1.24)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／１５５５２
(87)国際公開番号　ＷＯ９９／０５８１４
(87)国際公開日　平成11年２月４日(1999.2.4)
(31)優先権主張番号　６０／０５３，６６８
(32)優先日　平成９年７月24日(1997.7.24)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ワールドトーク・コーポレイション
アメリカ合衆国カリフォルニア州95054，サンタクララ，オールド・アイロンサイズ・ドライブ・5155
(72)発明者　ディッキンソン，ロバード，ディー，ザ・サード
アメリカ合衆国ワシントン州98053，レッドモンド，ノースイースト・フォーティフィフス・プレイス・23621
(72)発明者　クリシュナムルシー，サスヴィク
アメリカ合衆国カリフォルニア州95138，サンノゼ，キラーニー・サークル・5931
(74)代理人　弁理士　古谷　馨　（外２名）

最終頁に続く

(54)【発明の名称】　格納された鍵による暗号化／暗号解読を用いた電子メール用ファイアウォール

(57)【要約】
【課題】　組織に対して出入りするE-Mailﾒｯｾｰｼﾞに対する改善された中央制御を提供するE-Mailﾌｧｲｱｳｫｰﾙを提供すること。
【解決手段】　管理者選択可能な複数のﾎﾟﾘｼｰ(216)に従って第1ｻｲﾄと複数の第2ｻｲﾄとの間のE-Mailﾒｯｾｰｼﾞ(204)にﾎﾟﾘｼｰを適用するE-Mailﾌｧｲｱｳｫｰﾙ(105)。該ﾌｧｲｱｳｫｰﾙは第1ｻｲﾄと選択された第2ｻｲﾄとの間でE-Mailﾒｯｾｰｼﾞ(204)を送信させるSMTPﾘﾚｰ(202)を備える。複数のﾎﾟﾘｼｰﾏﾈｰｼﾞｬ(216)が管理者選択可能ﾎﾟﾘｼｰを強制実行する。暗号化及び暗号解除ﾎﾟﾘｼｰ等のﾎﾟﾘｼｰは、少なくとも1つの第1ｿｰｽ／ﾃﾞｽﾃｨﾈｰｼｮﾝﾎﾟﾘｼｰ(218)、少なくとも1つの第1ｺﾝﾃﾝﾂﾎﾟﾘｼｰ(220)、及び少なくとも1つの第1ｳｨﾙｽﾎﾟﾘｼｰ(224)を有する。該ﾎﾟﾘｼｰは複数の管理者選択可能基準(310)、該基準に対する複数の管理者選択可能例外(312)、及び該基準及び例外に関連する複数の管理者選択可能ｱｸｼｮﾝ(314,316,322)を特徴とする。



【特許請求の範囲】

【請求項１】

コンピューティングサイトから送信され又はコンピューティングサイトにより受信されたE-Mailメッセージを制御するためのE-Mail制御システムであって、

前記コンピューティングサイトから送信された第１の指定されたタイプのメッセージを少なくとも１つの第１の格納された暗号鍵に従って暗号化するメッセージ暗号化手段と、

前記コンピューティングサイトにより受信された第２の指定されたタイプのメッセージを少なくとも１つの第２の格納された暗号鍵に従って暗号解読するメッセージ暗号解読手段と、

該メッセージ暗号解読手段による暗号解読の後及び前記メッセージ暗号化手段による暗号化の前に、変更可能なフィルタ情報に従ってメッセージの監視を行う、フィルタとを備えている、E-Mail制御システム。

【請求項２】

前記フィルタがコンテンツフィルタを含み、該コンテンツフィルタが、その変更可能なコンテンツフィルタ情報に対応する情報を含むメッセージの送信を制限する、請求項１に記載のE-Mail制御システム。

【請求項３】

前記メッセージの各々が、該メッセージについての少なくとも１つの第１のデスティネーションを識別するデスティネーション情報を有しており、前記フィルタがデスティネーションフィルタを含み、該デスティネーションフィルタが、その変更可能なデスティネーションフィルタ情報に対応する情報を含むメッセージの送信を制限する、請求項２に記載のE-Mail制御システム。

【請求項４】

前記メッセージの各々が、該メッセージについての少なくとも１つの第１のソースを識別するソース情報を有しており、前記フィルタがソースフィルタを含み、該ソースフィルタが、その変更可能なソースフィルタ情報に対応する情報を含むメッセージの送信を制限する、請求項３に記載のE-Mail制御システム。

【請求項５】

前記フィルタに応じて、前記変更可能なフィルタ情報に対応する情報を含むメッセージを、該メッセージの少なくとも前記第１のデスティネーションとは異なるデスティネーションへ転送させる手段を備えている、請求項４に記載のE-Mail制御システム。

【請求項６】

前記フィルタに応じて、前記変更可能なフィルタ情報に対応する情報を含むメッセージを、該メッセージの少なくとも前記第１のデスティネーションに対応するデスティネーションへ転送させる手段を備えている、請求項５に記載のE-Mail制御システム。

【請求項７】

前記メッセージを転送させる前記手段に応じてE-Mail通知メッセージを生成させる通知手段と、

前記E-Mail通知メッセージを、変更可能な通知メッセージデスティネーション情報に対応するデスティネーションへ送信させる転送手段と

を備えている、請求項６に記載のE-Mail制御システム。

【請求項８】

前記通知メッセージが本体部分を有しており、前記通知手段が前記本体部分に含まれるメッセージを生成させる手段を備えている、請求項７に記載のE-Mail制御システム。

【請求項９】

１つの内部サイトと複数の外部サイトとの間で送信されるE-Mailメッセージを処理するためのE-Mailファイアウォールであって、

第１の外部サイトからのふるい分けされておらず暗号化されているE-Mailメッセージを受信し、及びふるい分けされており暗号化されているE-Mailメッセージを第２の外部サイトへと送信する、E-Mailリレーと、

前記第１の外部サイトから受信した前記ふるい分けされていない暗号化されたE-Mailメッセージに応じて、該メッセージを暗号解読し、第１の格納されている鍵に従って、ふるい分けされておらず暗号化されていないメッセージを生成し、ふるい分けされており暗号化されていないE-Mailメッセージに応じて、第２の格

納されている鍵に従って、前記ふるい分けされており暗号化されていないE-Mailメッセージを暗号化して、前記ふるい分けされており暗号化されているE-Mailメッセージを生成する、セキュリティマネージャと、

前記セキュリティマネージャにより生成された前記ふるい分けされておらず暗号化されていないE-Mailメッセージに応じて、該ふるい分けされておらず暗号化されていないE-Mailメッセージを、格納されているポリシー情報に従ってふるい分けして、ふるい分けされており暗号化されていないE-Mailメッセージを、該ふるい分けされており暗号化されていないE-Mailメッセージにより指定された第１の内部サイトのために生成し、及び第２の内部サイトからのふるい分けされておらず暗号化されていないE-Mailメッセージに応じて、該ふるい分けされておらず暗号化されていないE-Mailメッセージを、前記格納されているポリシー情報に従ってふるい分けして、前記セキュリティマネージャのために前記ふるい分けされており暗号化されていないE-Mailメッセージを生成する、ポリシーマネージャとを備えている、E-Mailファイアウォール。

【請求項１０】

１つの第１のサイトと複数の第２のサイトとの間のE-Mailメッセージの送信を、管理者により選択することが可能な複数のポリシーに従って制限するためのE-Mailファイアウォールであって、

前記第１のサイトと前記第２のサイトのうちの選択されたサイトとの間で前記E-Mailメッセージを送信させるためのＳＭＴＰ(Simple Mail Transfer Protocol)リレーと、

管理者により選択することが可能な複数のポリシーを前記ＳＭＴＰリレーに応じて強制的に実行するポリシーマネージャであって、前記ポリシーが、少なくとも１つの第１のソース／デスティネーションポリシーと、少なくとも１つの第１のコンテンツポリシーと、少なくとも１つの第１のウィルスポリシーとを有しており、該ポリシーが、管理者により選択することが可能な複数の基準と、管理者により選択することが可能な前記基準に対する複数の例外と、管理者により選択することが可能な前記基準及び前記例外に関連する複数のアクションとを特徴とするものである、ポリシーマネージャとを備えており、該ポリシーマネージャが

、

前記第１のサイトと前記第２のサイトとの間でのE-Mailメッセージの送信を前記ソース／デスティネーションポリシーに従って制限するアクセスマネージャと

、

前記第１のサイトと前記第２のサイトとの間でのE-Mailメッセージの送信を前記コンテンツポリシーに従って制限するコンテンツマネージャと、

前記第１のサイトと前記第２のサイトとの間でのE-Mailメッセージの送信を前記ウィルスポリシーに従って制限するウィルスマネージャと

を備えている、E-Mailファイアウォール。

【請求項１１】

前記ポリシーマネージャが、管理者により選択することが可能な前記ポリシーに応じて前記E-Mailメッセージを第１のフォーマットから第２のフォーマットへと変換するフォーマットマネージャを備えている、請求項１０に記載のE-Mailファイアウォール。

【請求項１２】

前記E-Mailメッセージが複数のフィールドへとフォーマットされ、該複数のフィールドが、ソースフィールド、デスティネーションフィールド、サブジェクトフィールド、、及びメッセージフィールドを含み、前記アクセスマネージャが、前記E-Mailメッセージの前記フィールドの各々毎に指定された前記ソース／デスティネーションポリシーに応答する、請求項１０に記載のE-Mailファイアウォール。

【請求項１３】

前記E-Mailメッセージがサイズフィールドを特徴とし、前記アクセスマネージャが、該サイズフィールドについて指定された前記ソース／デスティネーションポリシーに応答する、請求項に記載のE-Mailファイアウォール。

【請求項１４】

前記E-Mailメッセージが日付及び時間フィールドを特徴とし、前記アクセスマネージャが該日付及び時間フィールドについて指定された前記ソース／デスティネーションポリシーに応答する、請求項１２に記載のE-Mailファイアウォール。

【請求項１５】

前記ウィルスマネージャが、圧縮された情報を含むE-Mailメッセージに応じて該圧縮された情報中に含まれるウィルスを検出する、請求項１０に記載のE-Mailファイアウォール。

【請求項１６】

前記コンテンツマネージャが、前記コンテンツポリシーに従って、前記サブジェクトフィールド及び前記メッセージフィールドに含まれる情報に応答する、請求項１２に記載のE-Mailファイアウォール。

【請求項１７】

前記E-Mailメッセージが添付フィールドを含み、前記コンテンツマネージャが、前記コンテンツポリシーに従って、前記添付フィールドに指定された添付情報に応答する、請求項１６に記載のE-Mailファイアウォール。

【請求項１８】

１つの第１のサイトと複数の第２のサイトとの間のE-Mailメッセージの送受信を複数の変更可能なポリシーに従って制限するための方法であって、

前記第１のサイトと前記第２のサイトのうちの少なくとも１つとの間で送信された第１のE-Mailメッセージを傍受し、

前記メッセージが暗号化されているか否かを判定し、該メッセージが暗号化されている場合に、格納されている鍵に従って前記メッセージを暗号解読し、

複数の格納されているポリシーに従って前記メッセージのフィルタリングを行う、

という各ステップを有する、E-Mailメッセージの送受信を制限するための方法。

【請求項１９】

前記第２のサイトのうちの１つと前記第１のサイトとの間で送信された第２のE-Mailメッセージを傍受し、

該E-Mailメッセージを複数の格納されているポリシーに従ってフィルタリングし、

前記格納されているポリシーのうちの第１のポリシーに応じて前記格納されている鍵に従って前記E-Mailメッセージを暗号化し、

該E-Mailメッセージを前記第１のサイトに送信する、

という各ステップを更に有する、請求項１８に記載の方法。

【請求項２０】

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、一般に、コンピュータセキュリティ分野に関し、特に、電子メールシステムのためのセキュリティに関する。

【０００２】

【従来の技術】

インターネットの成長及び遍在に伴う電子メール(E-Mail)及びグループウェアの広範な用途により、業務レベル通信及び電子商取引(ＥＣ)のための新たな道が切り開かれた。組織は、組織内における購入注文、販売予測、財務情報、及び契約といった重要なファイルの伝送のためにインターネットを介したE-Mailに次第に依存するようになり、また異なる組織との間でも同様の処理のためにE-Mailに次第に依存するようになってきた。このような状況では、それらのファイルは、保護されなければならない重要な資産となっている。

【０００３】

現代のデータ通信の機密性及び保全性を保証するために、多数のセキュリティ基準が従来存在する。例えば、従来のファイアウォールは、権限のないユーザによるネットワークアクセスを防止する。セキュアソケット技術(Secure Socket Technology)は、ワールドワイドウェブ(WWW)を介してデータを安全に送ることを可能にする。しかし、インターネット上での最も突出した用途であるE-Mailは、殆どの組織にとってセキュリティという点で依然として問題の多いものである。多くの従来のファイアウォールは、単に該ファイアウォールにより保護されている情報へのアクセスを制限するものであり、E-Mailによる組織内外への情報の伝送を制限する能力は有していない。これは、組織内からE-Mailが発せられることによる機密情報の偶発的な又は意図的な開示、及び組織内に入ってきたE-Mailによるウィルス感染に通ずるものとなる。

【０００４】

気密性又はE-Mailメッセージを保護するための１つの方法として、かかるメッセージの暗号化が挙げられる。また、E-Mailメッセージの認証を提供するディジ

タル署名によりセキュリティを得ることができる。暗号化及び認証は、いずれも、Ｓ／ＭＩＭＥ（Secure/Multipurpose Internet Mail Extensions）メッセージングプロトコルでサポートされている。該プロトコルは、ＩＥＴＦ(International Engineering Task Force)により発行された「S/MIME Message Specification」(1997年)及び「S/MIME Certificate Handling」(1997年)と題する文書において規定されている。個々のユーザは、市販のソフトウェアを使用してE-Mailメッセージの暗号化／暗号解読及び認証を実施することができる。しかし、ソフトウェアを使用したかかる作業の実施は、常に単純なものとは限らず、それ故、通信手段としてのE-Mail本来の使用の容易性が損なわれることになり得る。更に、かかるソフトウェアを使用することを望む組織は、中央制御を行うための手段を何ら有することなく、必要となる全てのメッセージの暗号化を各ユーザに委ねなければならない。加えて、多くの従来のファイアウォールは、組織に出入りする一定のメッセージの内容又は形式を制御する能力を有していない。例えば、多くの従来のファイアウォールは、内容又はソース及び／又はデスティネーションアドレス又はドメインが暗号化されていること等の一定の基準をE-Mailが満たしていることを保証する能力を有していない。更に、多くの従来のファイアウォールは、組織内に入ってくる歓迎されないE-Mail広告等の望ましくないメッセージを制御する能力を有していない。

【０００５】

【発明が解決しようとする課題】

したがって、組織に対して出入りするE-Mailメッセージに対する改善された中央制御を提供するE-Mailファイアウォールが必要とされている。

【０００６】

【課題を解決するための手段】

主たる態様では、本発明は、コンピュータネットワーク(101,103)内で発生し又は同ネットワーク内へ入るE-Mailメッセージ(204)のふるい分けを行うE-Mailファイアウォール(105)を提供する。本発明の原理を採用した実施形態は、コンピューティングサイトとの間で送受信されるE-Mailメッセージ(204)の制御を行うE-Mail制御システム(105)という形を有利にとるものとなる。該E-Mail制御シ

ステム(105)は、少なくとも第１の格納された暗号鍵(528)に従って、コンピューティングサイトから送信された第１の指定されたタイプのメッセージ(204)の暗号化を行う、メッセージ暗号化手段(526)を備えている。メッセージ暗号解読手段(552)は、少なくとも第２の格納された暗号鍵(528)に従って、コンピューティングサイトにより受信された第２の指定されたタイプのメッセージ(204)の暗号解読を行う。フィルタ(216)は、前記メッセージ暗号解読手段(552)による暗号解読の後及び前記メッセージ暗号化手段(526)による暗号化の前に、変更可能なフィルタ情報(216)に従って、メッセージ(204)の監視を行う。

【０００７】

かかる実施形態の重要な利点は、組織によるE-Mailポリシーの中央制御が増大することにある。組織内へ入り又は組織内で発生した全てのE-Mailメッセージを、組織により課せられたポリシーに従って、暗号化し又は暗号解読し、及びフィルタリングすることができる。このため、組織内のデスクトップコンピュータの各ユーザは、該組織のE-Mailポリシーに確実に従うということに関わる必要がない。E-Mailメッセージは、特定の内容について、又は特定のソース若しくはデスティネーションについて、監視することが可能である。

【０００８】

有利にも、本発明の原理を採用した実施形態は、組織内の個々のユーザに対して透明な存在として作用するものとなる。例えば、かかる個々のユーザは、組織の暗号化ポリシーに従うことに関わる必要がない。特定の内容を含むE-Mailメッセージ、又は指定されたアドレス又はドメインから発せられ若しくは該アドレス又はドメインへと送信されるE-Mailメッセージを、自動的に暗号化し、及び／又はフィルタリングすることができる。例えば、他の組織（例えば会社Ｂ）と頻繁にE-Mailを交換する組織（例えば会社Ａ）が、会社Ｂへの全てのE-Mailがセキュリティ上暗号化されているべきであると判断した場合には、上述のような会社ＡにE-Mailファイアウォールを構築して、会社Ｂのドメインネームを認識し、及び暗号鍵を格納することが可能である。その後は、会社Ａから会社Ｂへの全てのE-Mailメッセージは、各ユーザによる付加的な操作を必要とすることなく、上述のE-Mailファイアウォールにより暗号化されることになる。会社Ｂが上述の原理を

採用したE-Mailファイアウォールを既に構築している場合には、該E-Mailファイアウォールは、会社Ａからのメッセージを暗号解読するよう構築することが可能である。よって、会社ＡからのE-Mailを受信した会社Ｂ内の各受信者は、会社ＡからのE-Mailを暗号解読するために付加的な操作を行う必要がない。したがって、会社Ａから会社Ｂへの全てのE-Mailメッセージは、会社Ａでも会社Ｂでもユーザによる介在なしに確実に交換することが可能となる。勿論、会社ＢのE-Mailファイアウォールは、会社Ｂから会社Ａへの同様のE-Mailメッセージ送信が可能となるように構成することが可能である。

【０００９】

更に、会社Ａ，Ｂ間のメッセージ伝送に対して別のポリシーを実施することが可能である。例えば、対象となるE-Mailファイアウォールの上述のフィルタを、特定の用語又はフレーズを含むE-Mailメッセージを認識してその伝送を防止するルールを用いて構成することにより、会社Ａ，Ｂ間における特定情報の偶発的な（又は意図的な）開示を低減させることが可能である。E-Mailファイアウォールはまた、かかるルールに対する例外を用いるように構成することも可能である。例えば、特定ユーザからのE-Mail又は特定ユーザへのE-Mailを、かかるルールの適用の対象外とすることが可能である。また、メッセージの伝送が阻止された後にE-Mailファイアウォールにより実行される動作は変更することが可能である。例えば、問題となるメッセージを説明メッセージと共に送信者に返すことが可能である。代替的に若しくは上記に加えて、管理者が見るために当該メッセージを格納すること、又は該メッセージを削除することが可能である。（１つ又は２つ以上のドメイン又は個々のアドレスにそれぞれ関連する）多数の暗号鍵を上述の原理を採用したE-Mailファイアウォールに格納して、多数のドメイン及び／又は個々のユーザとの安全な通信を可能にすることができる。

【００１０】

本発明の上述その他の利点については、以下の詳細な説明を参照することにより一層良好に理解されよう。

【００１１】

【発明の実施の形態】

図１において、E-Mailネットワーク101,102は、インターネット等のＷＡＮ(Wide Area Network)104を介してE-Mailネットワーク103に接続されている。インターネット104とE-Mailネットワーク101,103との間には、アクセスファイアウォール106及びE-Mailファイアウォール105が配設されている。E-Mailネットワーク102は、アクセスファイアウォール106のみによりインターネット104に接続されている。E-Mailネットワーク101,102,103はそれぞれ従来の形態をとるものである。例えば、E-Mailネットワーク101～103は、１つのＬＡＮ(Local Area Network)、又は１つ又は２つ以上の従来のE-Mailメッセージングプロトコルをサポートする複数のＬＡＮという形をとることが可能である。アクセスファイアウォール106もまた従来の形態をとることが可能である。アクセスファイアウォール106は、遠隔地に配置されたマシンからコンピュータネットワーク（E-Mailネットワーク101～103等）内に格納されているファイルへのアクセスを制限するよう動作する。E-Mailファイアウォール105（符号105.1及び105.2で別個に示す）は、１つの内部サイトと１つ又は２つ以上の外部サイトとの間のE-Mailメッセージの伝送を制御するために本書で詳細に説明するような形を有利にとることが可能である。E-Mailファイアウォール105.2に関する１つの内部サイトは、例えば、E-Mailネットワーク103という形をとることが可能である。E-Mailファイアウォール105.2に関する外部サイトは、E-Mailネットワーク103内に含まれないあらゆるサイトである。例えば、E-Mailファイアウォール105.2に関する外部サイトは、E-Mailネットワーク101,102内の任意のサイト、並びにインターネット104に接続された他のあらゆるサイトである。E-Mailファイアウォール105は、好適には、アクセスファイアウォール106の「安全な側」に配置される。図１は、例えば、本書に記載する実施形態の原理を示すものとして理解されるべきである。アクセスファイアウォール106は、本発明の例示目的で示されたものに過ぎず、本発明の原理を採用した実施形態の動作にとって必要なものではない。

【００１２】

好適には、E-Mailファイアウォール105は、従来の汎用コンピュータ上で実行されるプログラムという形をとる。典型的な実施形態では、コンピュータは、Microsoft Corporation (Redmond, Washington) から入手可能なWindows NT (商標

)オペレーティングシステムを実行する。図１では、E-Mailファイアウォール105は、内部サイトと外部サイトとの間でE-Mailメッセージに関して動作するものとして示されているが、該E-Mailファイアウォール105を使用して、ＳＭＴＰに従うメッセージングバックボーンを有する複数のコンピュータネットワークの２つの内部サイト間でメッセージを交換することも可能である。

【００１３】

図２は、E-Mailファイアウォール105.1,105.2の主な機能的な構成要素を示すブロック形式で示したものである。同図において、ＳＭＴＰ(Simple Mail Transfer Protocol)リレーモジュール202は、従来のインターネットリレーホストの機能を果たすものである。インターネットリレーホストの一例がsendmailプログラムである。ＳＭＴＰリレーモジュール202は、内部サイト210及び外部サイト212との間でE-Mailメッセージ（符号204で示す）の送受信を行う。E-Mailメッセージ204は、該メッセージ204のソースのE-Mailアドレスを指定するソースフィールド205、該メッセージ204の１つ又は２つ以上のデスティネーションE-Mailアドレスを指定するデスティネーションフィールド206、該メッセージ204の題名（即ちサブジェクト）を指定するサブジェクトフィールド207、該メッセージ204の本体（テキスト及び／又はグラフィクスデータを含む）を指定する本体フィールド208、及び該メッセージ204と共に送信すべき１つ又は２つ以上のファイルを指定する添付フィールド209といった、複数のユーザ指定情報フィールドを含む従来のE-Mailメッセージという形をとる。その他のユーザ指定フィールドとして、メッセージの優先度、送信側エージェントの識別子、及びメッセージの日時が挙げられるが、ユーザ指定フィールドはこれらに限定されるものではない。

【００１４】

E-Mailメッセージ204は、以下で詳述するような複数のエンコード形式のうちの１つに従ってエンコードすることが可能である。ＳＭＴＰリレーモジュール202は、インターネットＲＦＣ821により指定されているＳＭＴＰプロトコルに従ってE-Mailメッセージの送受信を行う従来のソフトウェアモジュールという形をとるのが好ましい。ＳＭＴＰプロトコルは、本発明にとって重要なものではなく、他の実施例では、ＳＭＴＰリレーモジュールを、ＦＴＰ(File Transfer Protoco

l)又はＨＴＴＰ(Hyper-Text Transfer Protocol)等の別の形式でメッセージの送受信を行うモジュールに置き換えることが可能である。

【００１５】

ＳＭＴＰリレーモジュール202は、ＤＮＳ(Domain Name System)を使用してメッセージの受信者への経路指定を決定するよう構成されることが好ましく、また代替的には、管理者により指定されたＳＭＴＰホストへメッセージを中継することが可能である。ＤＮＳが選択された場合、デフォルトＳＭＴＰホストは、ＤＮＳサービスが利用できない場合であってもメッセージの送信を可能にするために依然として指定することが可能である。経路指定オプションは、ドメイン単位でオーバーライドすることが可能である。ＳＭＴＰリレーモジュール202は、有利にも、特定のホストとの間の上り又は下り方向のＳＭＴＰ接続を制限することをことを可能にし、及び特定のＳＭＴＰホストとの間の接続を拒否することを可能にする。

【００１６】

図３は、ＳＭＴＰリレーモジュール202により受信された内部サイト210及び外部サイト212からのメッセージがポリシーエンジン214によって処理される態様を示したものである。ポリシーエンジン214は、ＳＭＴＰリレーモジュール202からのメッセージを受容し、該メッセージの送信者（ソース）205についての送信者ポリシーのリスト302を作成し、及び受信者ポリシーのリスト304,306,308を各受信者毎に作成することにより、該メッセージにどのポリシーが適用可能であるかを判定する。次いで、ポリシーエンジン214は、各ポリシーを適用するためにポリシーマネージャ216を呼び出す。異なるタイプのポリシーは、その適用に関する所定の優先度を有している。例えば、暗号解除ポリシーは、他のポリシーの前に適用され、これにより、メッセージの本体フィールド208について作用するポリシーが該本体中に含まれる内容にアクセスすることが可能になる。代替的な実施形態では、ポリシーが適用される順番は、システム管理者によって選択することが可能である。アクセスマネージャポリシーが暗号解読ポリシーの後に適用され、次いで他のポリシーマネージャが、メッセージに適用されるべきポリシーにより示唆される順番で繰り返し呼び出される。次いで、ポリシーエンジン214が

、ポリシーマネージャからの結果を受信し、該受信した結果に従ってメッセージをＳＭＴＰリレーモジュール202へ送信する。該ポリシーエンジン214により受信された結果は、本書中で詳述する処置、注釈、及び通知等のアクションから構成される。ポリシーエンジン214によるメッセージ204の処理結果は、複数の付加的なメッセージ（例えば、送信者、受信者、又はシステム管理者への通知）を生成するものとなる。好適な実施形態では、ポリシーエンジン214は、ディジタルコンピュータにより実行されるプログラムとして実施される。

【００１７】

ポリシーマネージャ216は、E-Mailファイアウォール105の管理者により入力されたポリシーを強制実行するよう動作することが可能である。ポリシーマネージャ216は、特定形態のE-Mailメッセージのために管理者により構成されたポリシーを強制実行するための複数のモジュールから構成されるのが好ましい。例えば、E-Mailファイアウォール105において、ポリシーマネージャ216は、アクセスマネージャ218、コンテンツマネージャ220、フォーマットマネージャ222、ウィルスマネージャ224、及びセキュリティマネージャ226を含む、複数のマネージャモジュールを実施する。ポリシーマネージャ216は、構成モジュール230を介して管理者によりインプットされた入力によって開発されるのが好ましい。構成モジュール230はまた、管理者により入力された情報に応じて、ＳＭＴＰリレーモジュール202及びポリシーエンジン214を構成するよう動作する。図２に示しここで説明するポリシーマネージャは、模範的な実施形態の例示のみを目的としたものである。他のタイプのポリシーマネージャもまた、本書に記載の原理内にあるものとして意図されている。

【００１８】

アクセスマネージャ218は、E-Mailの送信が禁止されたデスティネーション、又はE-Mailを受信することができないソース等のアクセス制御ポリシーの強制実行を提供する。アクセスマネージャ218はまた、管理者により決定された最大メッセージサイズを越えるメッセージ、又はサブジェクトフィールド207中に特定のワードを含むメッセージをフィルタリングすることができる。アクセスマネージャ218はまた、ユーザにより指定されたメッセージの優先度によりメッセージ

のフィルタリングを行うことができる。例えば、図７に関して以下で詳述するように、高優先度のメッセージを直ちに送る一方、低優先度のメッセージを待ち行列に入れることが可能である。アクセスマネージャ218はまた、メッセージの送信日及び／又は時刻によりメッセージのフィルタリングを行うことが可能である。例えば、１日のうちの特定の時間帯又は特定の日（例えば週末又は休日）に送信されたメッセージは、（例えばコンテンツマネージャ220により）その保持又は更なるフィルタリングを実施することが可能である。

【００１９】

コンテンツマネージャ220は、コンテンツ制御ポリシーの強制実行をサポートする。好適には、コンテンツマネージャ220は、(a)本体フィールド208中の特定のワード、(b)サブジェクトフィールド207又は本体フィールド208中の特定のワード、(c)添付フィールド209（その全て又は名称／タイプ）という基準のうちの１つ又は２つ以上によるフィルタリングをサポートする。コンテンツ制御ポリシー、及びその他の適当なポリシーは、特定のマテリアル（例えば特定の通知又は拒否）を必要とするよう指定することが可能である。ウィルスマネージャ224は、ウィルスに感染したE-Mail添付ファイルを検出することにより、ウィルス制御ポリシーの強制実行をサポートする。ウィルスマネージャ224は、PKZip、PKLite、ARJ、LZExe、LHA、及びMSCompressを含む複数の圧縮されたファイルフォーマット中に含まれるウィルスを検出するのが好ましい。ウィルスマネージャ224は、例えば、市販のウィルススキャンエンジンを使用することが可能である。ウィルスマネージャ224はまた、「クリーンメッセージ」、即ち、ウィルススキャンが実施されておりウィルスに感染していないことがわかっているメッセージについてポリシーを適用するのが好ましい。かかるメッセージには、ウィルスが検出されなかったことを示す「クリーンスタンプ」注釈が付与される。

【００２０】

フォーマットマネージャ222は、第１のフォーマットから第２のフォーマットへのE-Mailメッセージの変換を提供する。好適な実施形態では、フォーマットマネージャ222は、UUENCODEフォーマットからMIMEフォーマットへとメッセージを変換する。好適には、フォーマットマネージャ222は、他のポリシーマネージャ

によるメッセージ処理に先だってメッセージの変換を行う。

【００２１】

セキュリティマネージャ226は、複数のE-Mail暗号化ポリシーを強制実行するのが好ましい。好適には、セキュリティマネージャ226は、クライアントセキュリティ使用ポリシー、暗号保護ポリシー、プレーンテキストアクセスポリシー、及びデフォルトアクションポリシーを強制実行する。セキュリティマネージャ226はまた、ユーザに代わって、図５(b)に関連して以下に詳述するプロキシ暗号化及び署名ポリシーを適用する。

【００２２】

クライアントセキュリティ使用ポリシーは、特定のユーザがデスクトップで暗号化又は署名を行うべきことを指定する。このポリシーを強制実行すべきときを示すために追加の基準を設定することが可能である。例えば、ドメイン又はフルE-Mailアドレスによる会社のＣＥＯから会社の弁護士へのE-Mailを、暗号化又は署名を必要とするものに指定して、代理人－クライアント特権を強制実行し、及び暗号化ポリシーを保留することが可能である。更に、クライアントセキュリティ使用ポリシーを使用して、既に暗号化形式にあり他の基準をおそらく満たすメッセージは保存されるべきであること（換言すれば、E-Mailファイアウォール105による処理、修正、又は暗号解読を行わないこと）を指定することが可能である。プレーンテキストアクセスポリシーは、特定のタイプの指定されたメッセージの受信者としてE-Mailファイアウォール105が設計されることを必要とする。E-Mailファイアウォール105は、アクセス、コンテンツ、ウィルスその他のポリシーをメッセージに適用するために、暗号化メッセージの受信者として指定される。プレーンテキストアクセスポリシーはまた、メッセージの送信者にE-Mailファイアウォール105の公開鍵を提供する１つの方法として署名付き通知をメッセージの送信者に送るために使用することが可能である。デフォルトアクションポリシーは、暗号化されていないメッセージであってE-Mailファイアウォール105により暗号化されることもなく且つ随意選択的に他の何らかの基準を満たすメッセージについて実行すべきアクションを示す。このポリシータイプは、特定のメッセージがどこかで（デスクトップで又はE-Mailファイアウォール105により）暗

号化されることを確実にするために使用される。

【００２３】

ポリシーは、許可された管理者により構成モジュール230を介して入力されるのが好ましく、該構成モジュール230は、プログラムが格納されたコンピュータ上で実行されるプログラムという形をとるのが好ましい。ポリシーは、ユーザに対して、個別に又はE-Mailドメイン若しくはその他のグループにより有利に適用することが可能である。図４は、ポリシーが適用される態様を示している。ユーザは、ユーザ及び／又はドメインのグループ化が容易となるように階層状のディレクトリ構造で編成することが可能である。所与のディレクトリにポリシーが適用される場合には、該所与のディレクトリに対応するサブディレクトリがかかるポリシーを受け継ぐ。例えば、図４において、ポリシー1は、サブディレクトリ404に適用され、ひいては全てのサブディレクトリ、ドメイン、及びユーザ（例えば、サブディレクトリ412、ユーザ408、及びドメイン410）に適用される。これは、該ポリシーが、特定のサブディレクトリ又は介在するサブディレクトリに適用された別のポリシーにより明示的にオーバーライドされない限り行われる。例えば、ポリシー3は、ユーザ1（符号408で示す）について、該ポリシー3とポリシー1との間に競合が存在する場合にはポリシー1をオーバーライドし、競合が存在しない場合にはポリシー1を補うことになる。例外1は、例外1で指定される特定の例外についてポリシー1,3をオーバーライドすることになる。図４に示すように、ポリシー1は、ユーザ414,416,418に適用され、競合が存在する場合にはユーザ414,416,418についてポリシー2によりオーバーライドされ、競合が存在しない場合には補足を行うことになる。これにより、ポリシーをユーザグループに容易に適用することが有利にも可能となる。ただし、ポリシーが格納される正確な態様は本発明にとって重要ではなく、様々な格納手段及び格納形式を採用することが可能である。

【００２４】

ＳＭＴＰリレーモジュール202により受信され及び／又は送信されたE-Mailメッセージ204は、ＩＥＴＦ(Internet Engineering Task Force)により「S/MIME Message Specification」(1997)及び「S/MIME Certificate Handling」(1997)と

題する文書中で指定されたＳ／ＭＩＭＥ(Secure/Multipurpose Internet Mail Extension)プロトコルに従ってエンコードされるのが好ましい。有利なことに、このＳ／ＭＩＭＥプロトコルは、RSA Data Security, Inc. により指定されたPublic Key Cryptography Standards (PKCS：公開鍵暗号化規格)に従う工業規格ＭＩＭＥプロトコルの最上層でセキュリティを構築する。Ｓ／ＭＩＭＥは、ディジタル証明書を用いた認証や暗号化を用いたプライバシーに関するセキュリティサービスを有利にも提供する。ディジタル証明書は、「ITU-T推奨X.509」(1997年6月)としても知られる「Information Technology - Open Systems Interconnection - The Directory:Authentication Framework」で指定されたX.509フォーマットに従って実施されるのが好ましい。暗号化は、対称暗号化アルゴリズムDES、Triple-DES、及びRC2のうちの１つにより実行されるのが好ましい。Ｓ／ＭＩＭＥプロトコルは、周知のものであり、広く使用されており、暗号化及びディジタル署名を提供するものであり、したがって通信プロトコルとして好適なものである。ただし、該プロトコルの動作の詳細は本発明にとって重要ではない。更に、ITFワーキンググループにより指定されたＰＧＰ(Pretty Good Privacy)又はOpenＰＧＰといった他の安全なメッセージングプロトコルを利用することも可能であることが理解されよう。

【００２５】

アクセスマネージャ218は、E-Mailメッセージ204を処理するための最初のポリシーマネージャである。アクセスマネージャ218は、暗号化されていないメッセージヘッダ情報についてのみ作用する。このため、アクセスマネージャ218は、Ｓ／ＭＩＭＥエンジン215による暗号解読に先立ってE-Mailメッセージ204を処理する。なお、用語「メッセージヘッダ情報」は、メッセージのうち本体フィールド208（一般にメッセージテキストとも呼ばれる）及び添付フィールド209を除いた部分を一般に指すものである。従って、ヘッダ情報は、ソースフィールド、デスティネーションフィールド、及びサブジェクトフィールド (205,206,207)を含んでいる。メッセージヘッダに含むことが可能な他のフィールドとしては、日付／時刻スタンプ、優先度、及び送信側エージェントが挙げられる。残りのモジュールは、Ｓ／ＭＩＭＥエンジン215による処理の後にメッセージ204に作用する。

既述のように、フォーマットマネージャ222は、ウィルスマネージャ224、セキュリティマネージャ226、及びコンテンツマネージャ220といった他のマネージャによる作用に先立ってメッセージに作用するのが好ましい。

【００２６】

Ｓ／ＭＩＭＥプロトコルは、Ｓ／ＭＩＭＥプロトコルをサポートする２つのサイトが安全なE-Mailメッセージ204の交換を行うことを可能にする。送信サイト及び受信サイトがＳ／ＭＩＭＥ機能を実行する場合には、図５(a)に示すような仮想プライベートネットワーク(ＶＰＮ)を達成することができる。結果的に得られるＶＰＮ（ここでは「オブジェクトレベルE-MailＶＰＮ」と称す）は、送信サイトと受信サイトとの間におけるメッセージの暗号化／署名、及び／又は、暗号解読／検証を提供する。図５(a)に示すオブジェクトレベルE-MailＶＰＮでは、各オブジェクト（メッセージ）は、個々に暗号化され、標準的な(ＳＭＴＰ)伝送媒体を介して送られる。この場合、各オブジェクトは他端で暗号解読される。有利なことに、該オブジェクトレベルE-MailＶＰＮは、従来のＶＰＮにより必要とされた安全なリアルタイム接続を必要としない。図５(a)に示すように、メールサーバ105.1,105.2は、E-Mailファイアウォール105に関して本書で説明した機能を実行し、その結果として、それらの間にオブジェクトレベルE-MailＶＰＮが達成される。メールサーバ105.1,105.2感で暗号化され送信されたE-Mailは、インターネット104を介して送信されたE-Mailが膨大な安全でないサーバを通過した後にそのデスティネーション（即ち宛先）に到達するという事実にもかかわらず、第三者に対する開示から保護される。かかる交換において、E-Mailファイアウォール105.1,105.2は、一対の鍵及び鍵証明書の生成を提供し、及び他のＳ／ＭＩＭＥサーバとの自動又は手動での公開鍵証明書の交換を提供する。加えて、E-Mailファイアウォール105.1,105.2は、ディレクトリドメインレコードを介した他のＳ／ＭＩＭＥサーバの識別、サーバ証明書とのディレクトリドメインレコードの結合、及び暗号化／署名アルゴリズム及び鍵長さの選択を可能にする。ディレクトリドメインレコード、及び以下で説明するディレクトリユーザレコードは、図４に記載されている。

【００２７】

Ｓ／ＭＩＭＥエンコード済みメッセージの交換はまた、E-Mailファイアウォール105.1,105.2と、Ｓ／ＭＩＭＥ機能を実行しないサーバに接続されたＳ／ＭＩＭＥクライアントとの間で実行することも可能である。図５(b)は、E-Mailファイアウォール105と非Ｓ／ＭＩＭＥサーバ506に接続されたＳ／ＭＩＭＥクライアントとの間のデータ交換を示している。図５(b)において、サーバ105.1は、クライアント502に代わってメッセージの暗号化及び暗号解読を行い、またE-Mailファイアウォール105.1,105.2に関する上述の機能を一般に提供する。詳細には、かかる交換では、E-Mailファイアウォール105.1は、一対の鍵及び公開鍵証明書の生成を提供し、及びクライアント508.1との自動又は手動での公開鍵証明書の交換を提供する。加えて、E-Mailファイアウォール105.1は、ディレクトリユーザレコードを介したクライアント508.1の識別、ユーザ証明書とのディレクトリユーザレコードの結合、及び暗号化／署名アルゴリズム及び鍵長さの選択を可能にする。クライアント508.1は、暗号化／暗号解読サービスをサポートすることによりサーバ506を介してメッセージを安全に送信することを可能にするために、暗号化／暗号解読サービスを提供する。図５(b)では、サーバ105.1とクライアント508.1との間に特定のタイプのオブジェクトレベルＶＰＮ（ここでは「プロキシセキュリティ」と称す）が達成される。プロキシセキュリティでは、少なくとも１つのクライアント（図５(b)中のクライアント508.1等）が暗号化／暗号解読の実行に関わる。これは、サーバ105.1,105.2により実行される暗号化／暗号解読サービスがクライアント502.1,502.2からは見えない図５(a)の構成とは対照的である。

【００２８】

図5(a)において、サーバ105.1,105.2間の通信は安全であるが、クライアント502.1,502.2とそれぞれのサーバ105.1,105.2との間の通信は安全でない。多くのかかる設備の場合、セキュリティは不要である。しかし、かかるセキュリティが望まれる場合には、クライアント508.1,508.2にも暗号化／暗号解読サービスを実装して、プロキシセキュリティを実行することが可能である。図５(c)におけるサーバ105.1,105.2は、図５(a)に関して上述したものと同じ機能を実行し、したがってオブジェクトレベルＶＰＮを達成する。加えて、クライアント508.2,50

8.1は、対応するサーバ105.1,105.2との間での安全な通信を可能にする。サーバ105.1,105.2により実行される暗号化／暗号解読は、対応するクライアント508.2,508.1により実行される暗号化から独立したものとすることが可能であることに留意されたい。例えば、クライアント508.2からクライアント508.1へのメッセージは、サーバ105.1への送信時に暗号化され、サーバ105.1により暗号解読され、ポリシーマネージャによる適当なアクションを受け、次いでサーバ105.2への送信のために暗号化され、サーバ105.2により暗号解読され、ポリシーマネージャによる適当なアクションを受け、次いでクライアント508.1への送信のために暗号化され、該クライアント508.1がメッセージを暗号解読する、といったことが可能である。代替的には、クライアント508.2からクライアント508.1へのメッセージは、クライアント508.2により暗号化され、非暗号化部分（デスティネーションフィールド等）に対する適当なアクションを受け、次いでメッセージ全体（クライアント508.2により暗号化されていない部分を含む）がサーバ105.2への送信のために再びサーバ105.1により暗号化され、該サーバ105.2がサーバ105.1による暗号化を解読し、クライアント508.2により実行された暗号化を解読するためにクライアント508.1へメッセージを送信することが可能である。上記２つのシナリオの組み合わせもまた実施可能である。

【００２９】

E-Mailファイアウォール105により処理された各E-Mailメッセージ204は、図６(a)及び図６(b)に示すステップに従って処理される。図６(a)は、受信したメッセージに応じたE-Mailファイアウォール105の動作を示すフローチャートである。図６(b)は、メッセージを送信する前のE-Mailファイアウォール105の動作を示すフローチャートである。E-Mailファイアウォール105により処理されたメッセージは、内部サイトへ送信するために内部サイトから受信し、又は外部サイトへ送信するために内部サイトから受信し、又は内部サイトへ送信するために外部サイトから受信する可能性のあるものである。あらゆる単一のメッセージは、内部及び外部デスティネーション206を含むことが可能である。図６(a)及び図６(b)に示すステップは、図３に示す送信者ポリシー及び受信者ポリシーを生成することにより実行される。従って、複数のデスティネーションの各々毎に、図６(b)

に示すステップは、様々に実行することが可能なものであり、異なるデスティネーション毎に異なる結果を有するものとなる。

【００３０】

ここで図６(a)を参照する。ステップ602で、E-Mailファイアウォール105は、メッセージ204の部分の暗号解読が必要であるか否かを判定する。暗号解読が必要である場合には、ステップ604で、格納されている鍵628に従って暗号解読が実行される。該暗号解読の後、又は暗号解読が不要であった場合には、E-Mailファイアウォール105がポリシーマネージャ216を適用し、該ポリシーマネージャ216が４つのタイプのアクション（ステップ610,612,614,616で示す）をE-Mailメッセージ204に対して実行する。基準アクション610は、管理者により選択されたフィルタリング基準を提供する。例外アクション612は、どの基準610が除外されているかを判定する。複数の基準610を選択することが可能であり、結果的に基準の論理ＡＮＤ演算が生じることになる。また複数の例外612を選択することが可能であり、結果的に例外の論理ＯＲ演算が生じることになる。即ち、例外条件のうちのいずれか１つが真であると、ポリシーはトリガされないことになる。注釈アクション614は、メッセージ204に対する添付フィールドの生成、又はメッセージ204の本体208中へのテキストの挿入を生じさせる。注釈アクションの実行態様は、管理者により入力されたポリシーに基づくものとなる。通知アクション616は、所与のポリシーがトリガされた際に１つ又は２つ以上のE-Mail通知の伝送を生じさせる。通知は、送信者、受信者、管理者、又は管理者により規定されたE-Mailアドレスへと伝送することが可能である。加えて、通知アクション616は、オリジナルメッセージ204を通知に添付すべきか否かに関する記述を可能にする。処置アクション620は、メッセージを（デスティネーションフィールド206により指定された）デスティネーションへ送り続けるべきか否か、又は複数の代替アクション622（メッセージの延期、隔離、送信者への返送、中止等）のうちの１つが必要であるか否かを判定する。

【００３１】

図６(b)に示すステップは、メッセージ204について指定された各デスティネーション毎に実行される。図６(b)に示すステップはまた、ステップ622により生成

されたメッセージについて実行される。第１に、ポリシーマネージャ216が、メッセージ204中で指定されている各デスティネーション毎にアクション610,612,614,616を実行する。処理アクション623は、メッセージを（デスティネーションフィールド206により指定された）デスティネーションへ送り続けるべきか否か、又は（メッセージの延期、隔離、送信者への返送、中止等）複数の代替アクション622のうちの１つ又は延期が必要であるか否かを判定することにより、処置アクション620と同様に動作する。ステップ624で、メッセージの暗号化が必要であるか否かが判定される。メッセージの暗号化が必要である場合には、ステップ626で、格納されている鍵628に従って暗号化が行われる。メッセージの暗号化が必要でない場合には、ステップ630で、指定されたデスティネーションへメッセージが送信される。また、ブロック622により処理されたメッセージは、送信前にステップ624でチェックされる。例えば、延期され、隔離され、又は送信者へ返送されるメッセージは暗号化を必要とする可能性がある。

【００３２】

図７は、代替アクション622を更に詳細に示すブロック図である。処置ステップ620から受信したメッセージは、指定されたメッセージ処置に応じて、隔離待ち行列704、リトライ待ち行列706、デッドレター待ち行列708、及び延期待ち行列709を含む４つの待ち行列702のうちの１つに格納される。隔離待ち行列704は、システム管理者その他の権限を有する人間による後続の取り出し及び検討に備えてメッセージを格納する。リトライ待ち行列706は、配信に失敗したメッセージを格納する。リトライ待ち行列706中のメッセージの送信は後に再試行される。デッドレター待ち行列708は、何回かの再試行の後に配信不能であり続け、送信者へ返送することもできないメッセージを格納する。デッドレター待ち行列708中のメッセージは、システム管理者によって処理されることになる。延期待ち行列709は、時期を遅らせて（例えば週末又は夜間等のピーク時期を外した時間に）自動的に配信されるべきメッセージを格納する。構成モジュール230は、待ち行列702中のメッセージについて実行することが可能な複数のアクション710～714を提供する。メッセージは、管理者が見ること（ブロック710）、送信者へ返送すること(ブロック711)、削除すること(ブロック712)、指定された１つ又は複

数のデスティネーションへ送ること(ブロック713)、及び／又はセーブすること(ブロック714)が可能である。

【００３３】

上述の特定の機構及び技術は、単に本発明の原理の一適用例を例示したものであることが理解されよう。本発明の真の技術的思想及び範囲から逸脱することなく上記の方法及び装置に様々な修正を加えることが可能である。

【図面の簡単な説明】

【図１】

インターネットを介して接続され本発明の原理を採用したE-Mailファイアウォールを使用した複数のE-Mailネットワークを示すブロック図である。

【図２】

E-Mailファイアウォールの好適な実施形態を示すブロック図である。

【図３】

図２のE-Mailファイアウォールの動作をより詳細に示すブロック図である。

【図４】

図２のE-Mailファイアウォールの動作をより詳細に示すブロック図である。

【図５(a)】

代替的な安全なE-Mail通信機構を示すブロック図である。

【図５(b)】

代替的な安全なE-Mail通信機構を示すブロック図である。

【図５(c)】

代替的な安全なE-Mail通信機構を示すブロック図である。

【図６(a)】

E-Mailファイアウォールの好適実施形態の動作を示すフローチャートである。

【図６(b)】

E-Mailファイアウォールの好適実施形態の動作を示すフローチャートである。

【図７】

図６(a)及び図６(b)の部分を一層詳細に示すブロック図である。

【符号の説明】

105 E-Mailファイアウォール

202 ＳＭＴＰリレーモジュール

204 E-Mailメッセージ

205 ソースフィールド

206 デスティネーションフィールド

207 サブジェクトフィールド

208 本体フィールド

209 添付フィールド

210 内部サイト

212 外部サイト

214 ポリシーエンジン

216 ポリシーマネージャ

218 アクセスマネージャ

220 コンテンツマネージャ

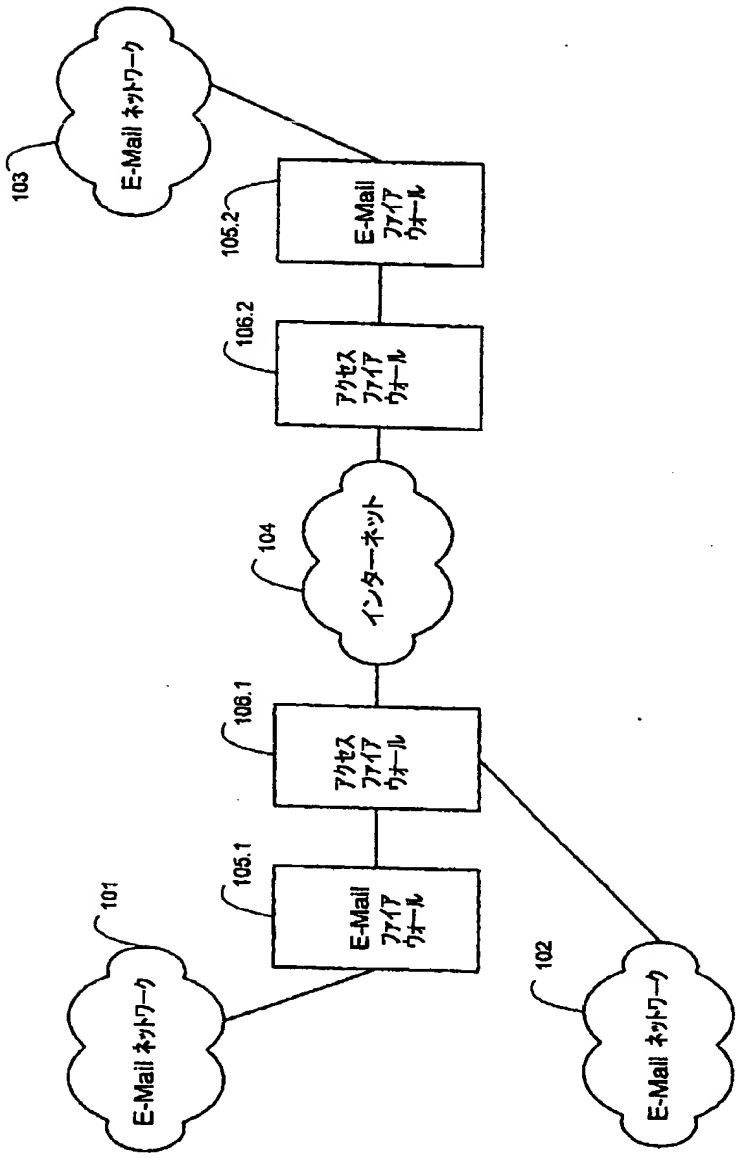
222 フォーマットマネージャ

224 ウィルスマネージャ

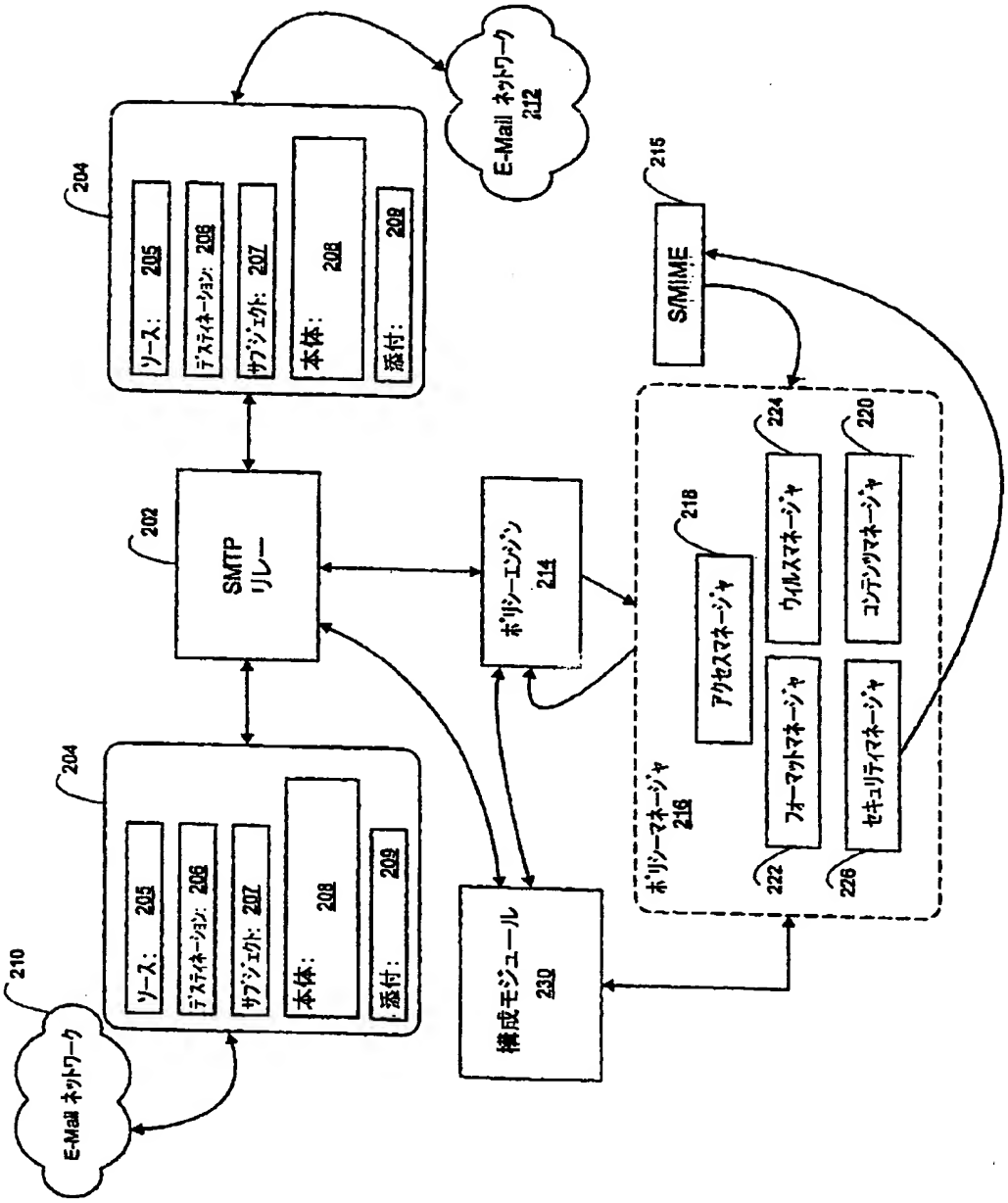
226 セキュリティマネージャ

230 構成モジュール

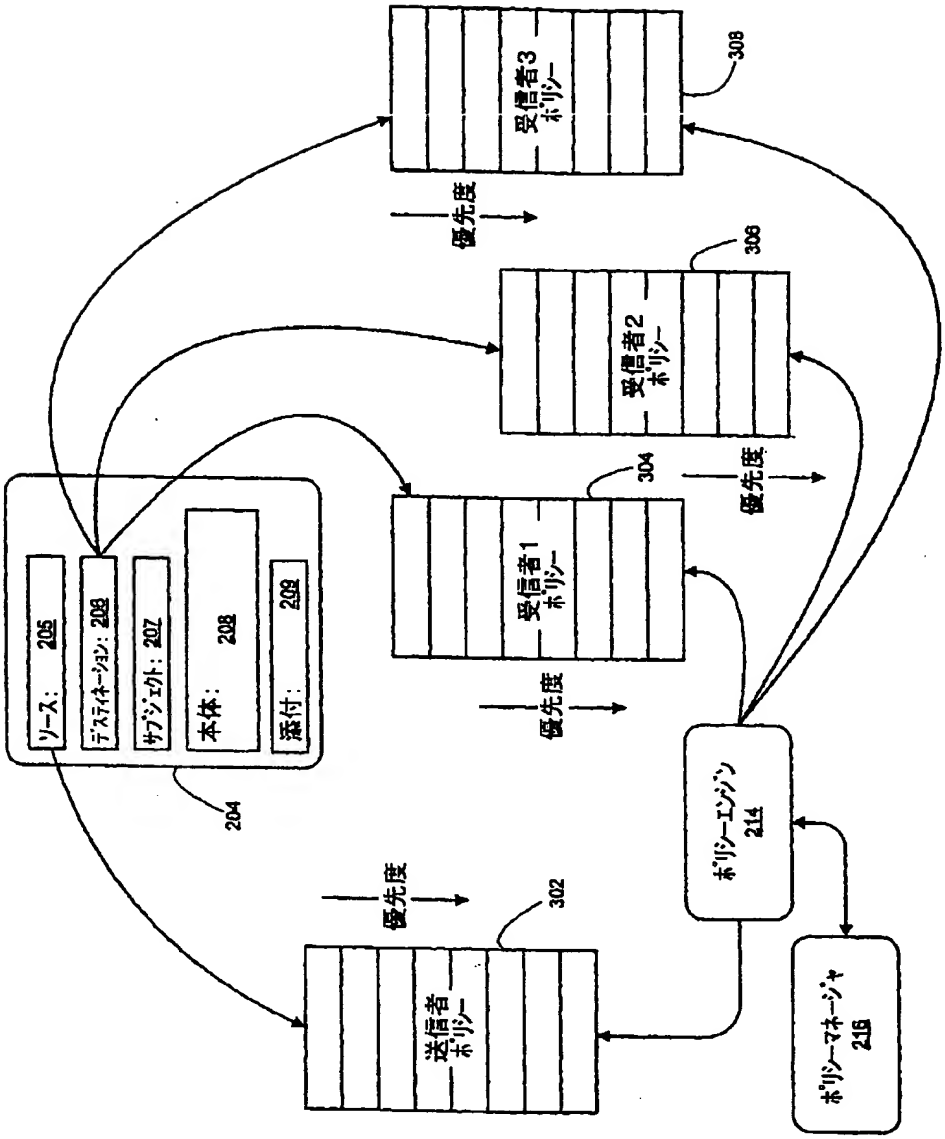
【図１】


E-Mail ネットワーク
103
105.2
E-Mail ファイア ウォール
106.2
アクセス ファイア ウォール
104
インターネット
106.1
アクセス ファイア ウォール
105.1
E-Mail ファイア ウォール
101
E-Mail ネットワーク
102
E-Mail ネットワーク

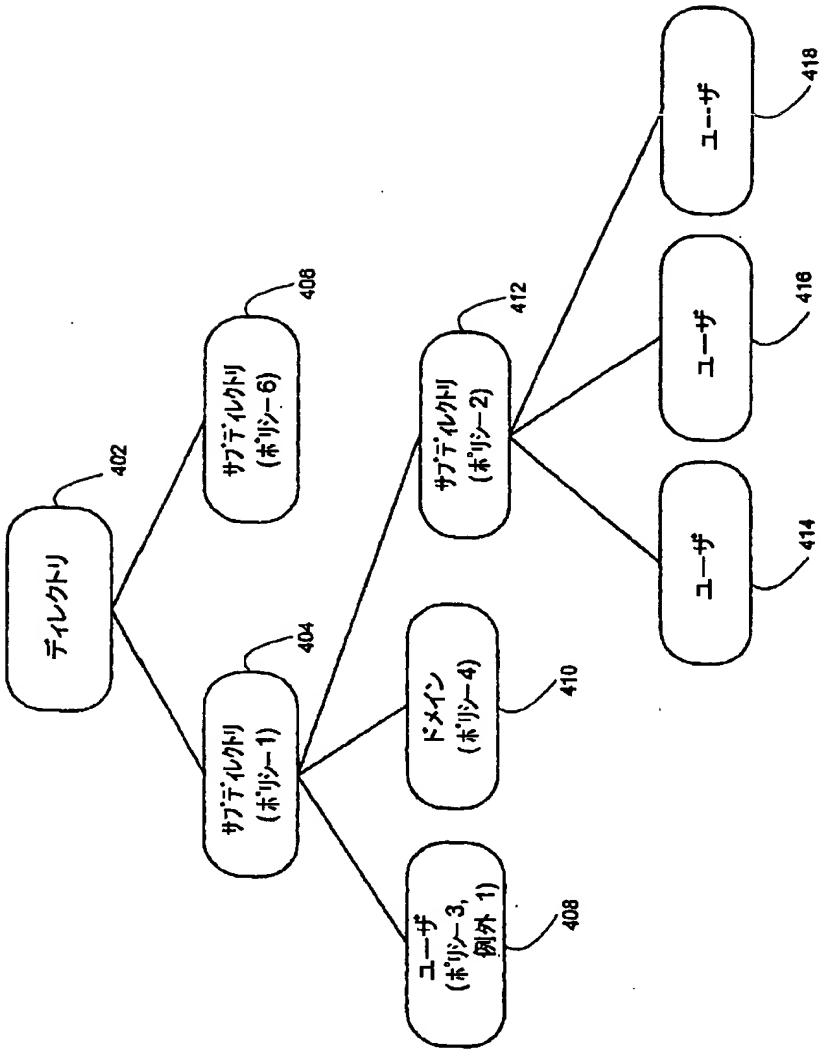
【図２】


E-Mail ネットワーク
212
204
ソース: 205
デスティネーション: 206
サブジェクト: 207
本体: 208
添付: 209
SMTP リレー
202
ポリシーエンジン 214
S/MIME
215
ポリシーマネージャ 216
アクセスマネージャ
218
ウイルスマネージャ
224
コンテンツマネージャ
220
フォーマットマネージャ
222
セキュリティマネージャ
226
構成モジュール 230
E-Mail ネットワーク
210

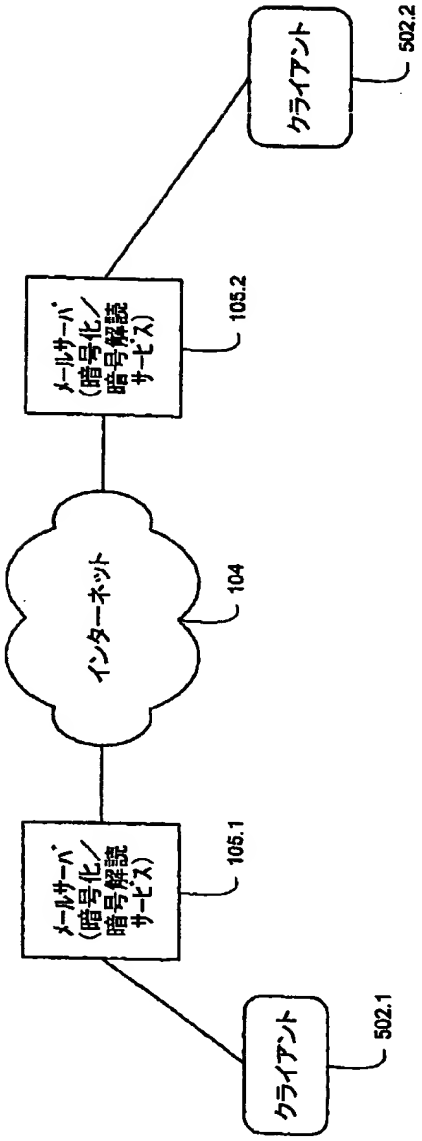
【図３】


受信者3 ポリシー
308
優先度
受信者2 ポリシー
306
受信者1 ポリシー
304
優先度
優先度
ソース: 205
デスティネーション: 206
サブジェクト: 207
本体: 208
添付: 209
204
ポリシーエンジン 214
優先度
送信者 ポリシー
302
ポリシーマネージャ 216

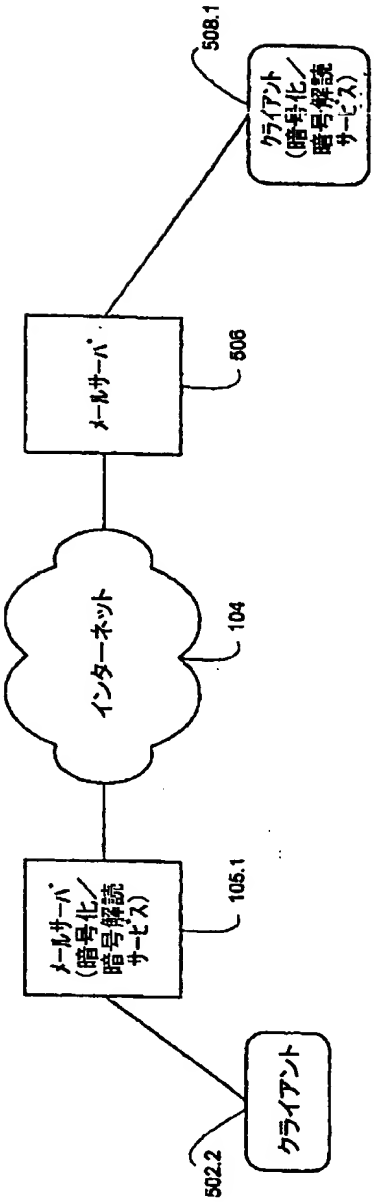
【図４】


ディレクトリ
402
サブディレクトリ (ポリシー6)
406
サブディレクトリ (ポリシー1)
404
ドメイン (ポリシー4)
410
ユーザ (ポリシー3, 例外1)
408
サブディレクトリ (ポリシー2)
412
ユーザ
418
ユーザ
416
ユーザ
414

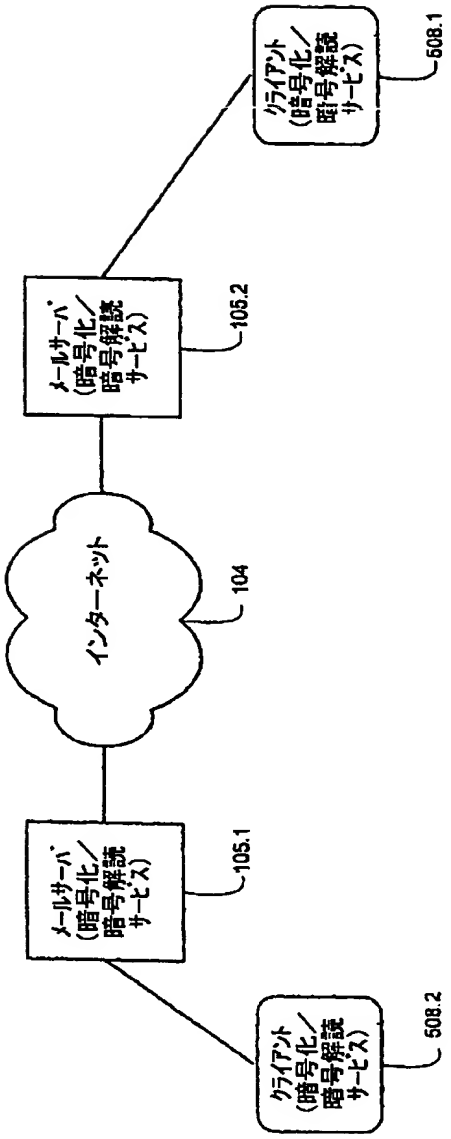
【図５（ａ）】


クライアント
502.2
メールサーバ
(暗号化/
暗号解読
サービス)
105.2
インターネット
104
メールサーバ
(暗号化/
暗号解読
サービス)
105.1
クライアント
502.1

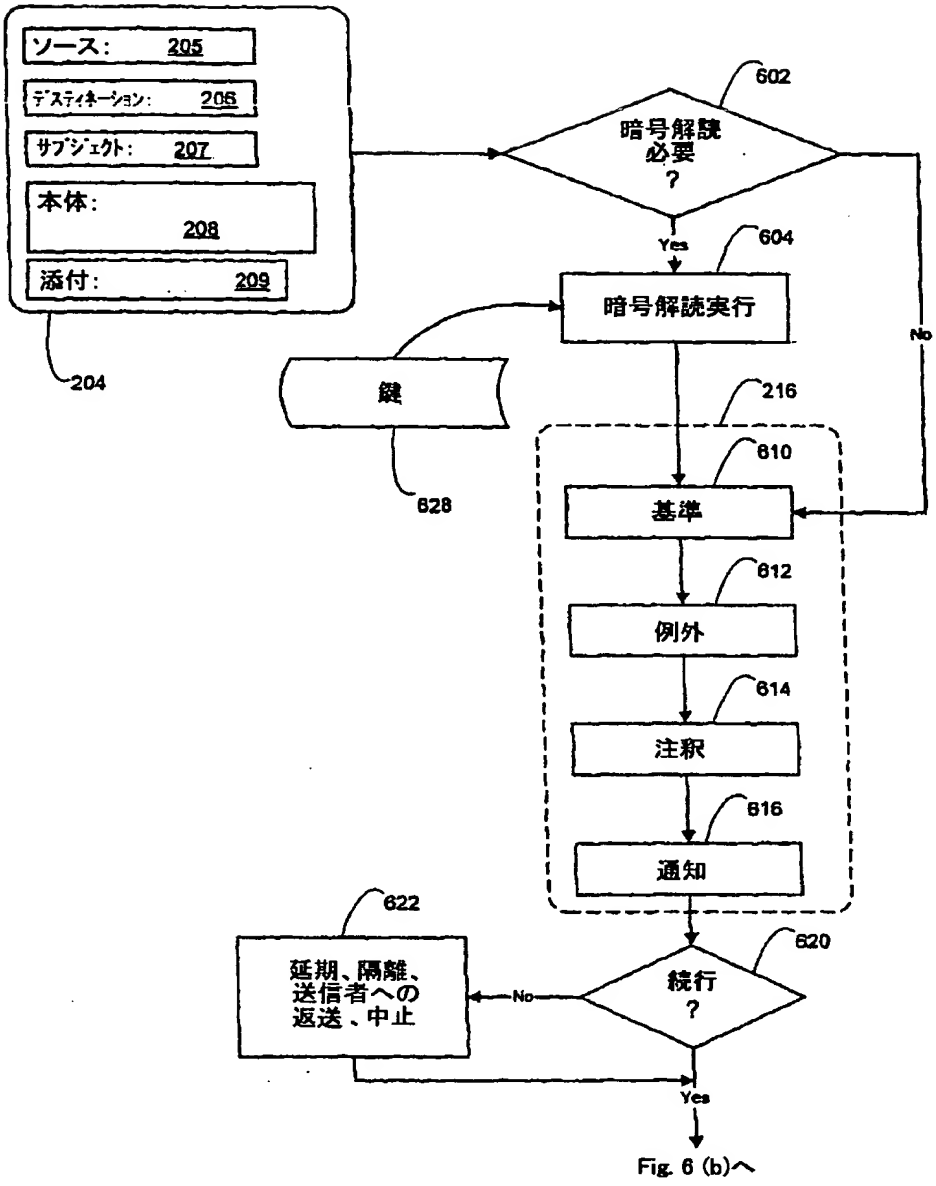
【図５（ｂ）】


508.1
クライアント（暗号化／暗号解読サービス）
メールサーバ
506
インターネット
104
メールサーバ（暗号化／暗号解読サービス）
105.1
クライアント
502.2

【図５（ｃ）】


クライアント
(暗号化／
暗号解読
サービス)
608.1
メールサーバ
(暗号化／
暗号解読
サービス)
105.2
インターネット
104
メールサーバ
(暗号化／
暗号解読
サービス)
105.1
クライアント
(暗号化／
暗号解読
サービス)
508.2

【図６（ａ）】


ソース: 205
ﾃﾞｽﾃｨﾈｰｼｮﾝ: 206
ｻﾌﾞｼﾞｪｸﾄ: 207
本体: 208
添付: 209
204
602
暗号解読必要？
Yes
No
604
暗号解読実行
鍵
628
216
610
基準
612
例外
614
注釈
616
通知
620
続行？
No
622
延期、隔離、送信者への返送、中止
Yes
Fig. 6 (b)へ

【図６（ｂ）】

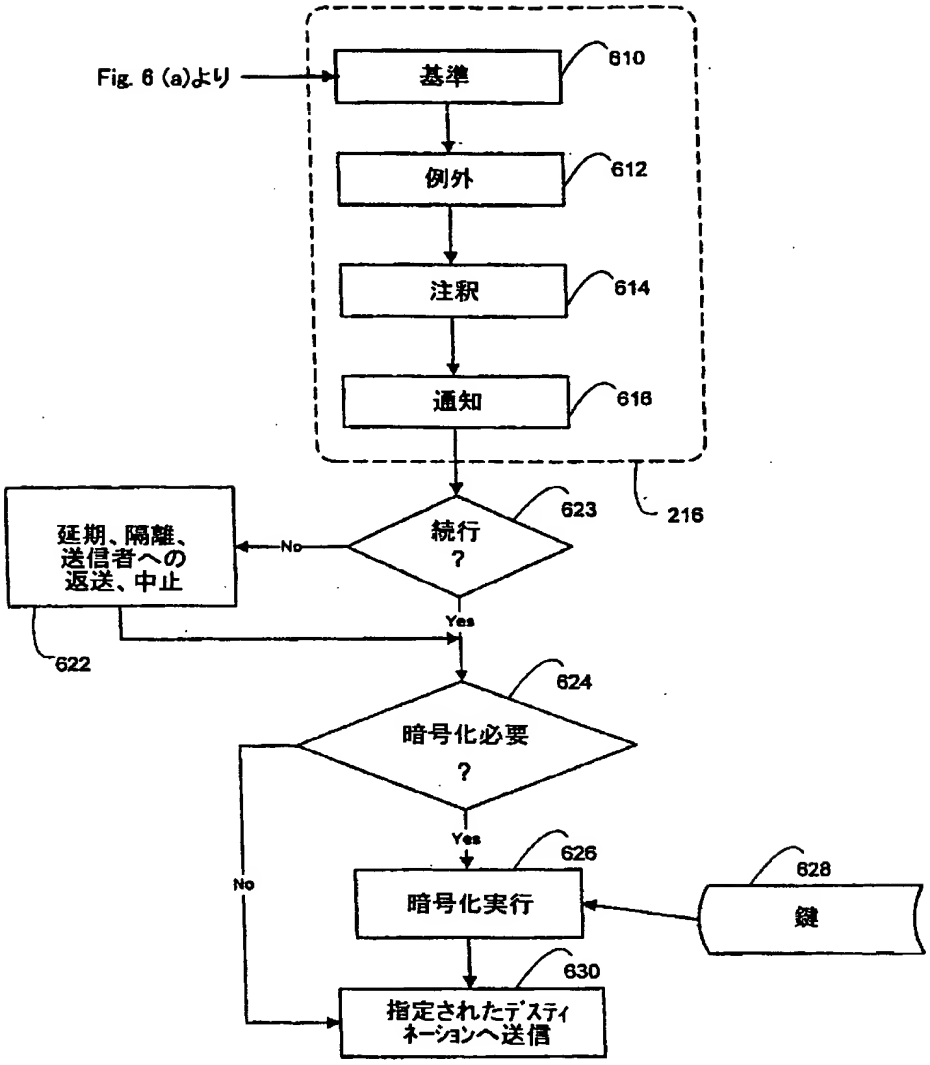
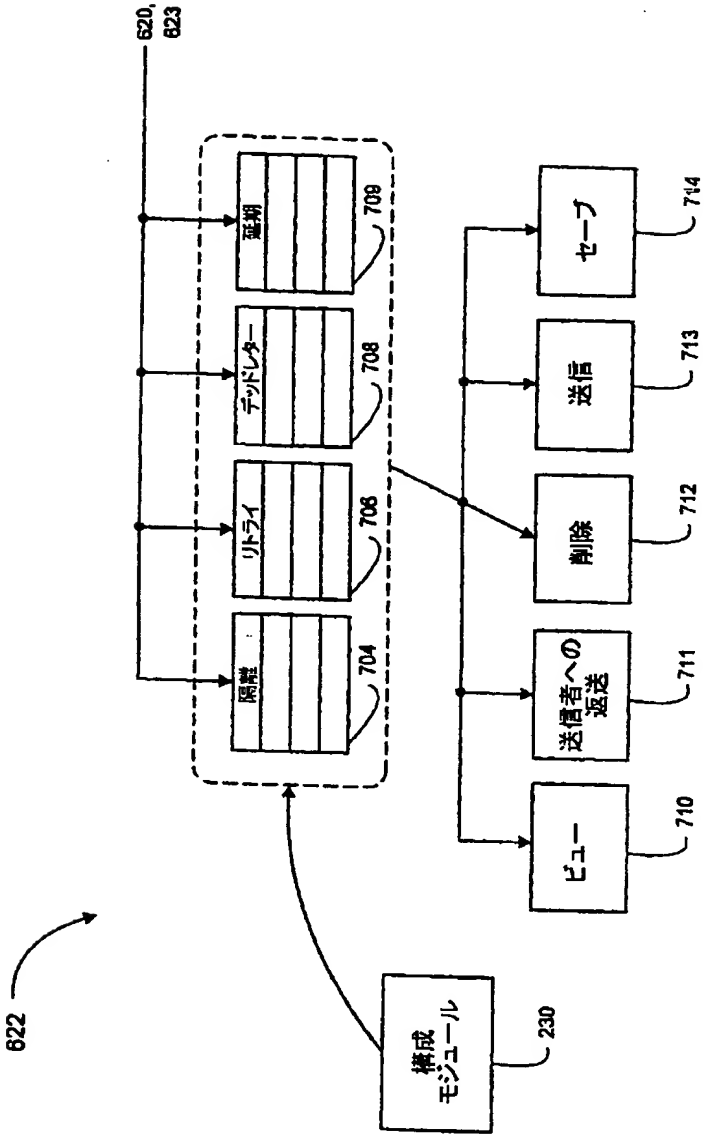


Fig. 6 (a)より
基準
610
例外
612
注釈
614
通知
616
216
623
続行
？
No
延期、隔離、
送信者への
返送、中止
622
Yes
624
暗号化必要
？
Yes
No
626
暗号化実行
628
鍵
630
指定されたﾃﾞｽﾃｨ
ﾈｰｼｮﾝへ送信

【図７】


620,
623
遅延
709
デッドレター
708
リトライ
706
隔離
704
セーブ
714
送信
713
削除
712
送信者への返送
711
ビュー
710
構成モジュール
230
622

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/15552

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) : H04K 1/00
US CL : 380/25
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25 395/all 380/all 364/all

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
EPO File, JPO File

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IETF Website: Archive

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,416,842 A (AZIZ) 16 May 1995 AB col. 5, lines 50-55, 59-61, 40-48 col. 11, lines 20-23	1-8, 10-19
Y	US 5,748,884 A (ROYCE et al.) 05 May 1998 col. 3, lines 39-42	7-8
Y	US 5,627,764 A (SCHUTZMAN et al.) 06 May 1997 col. 1, lines 36-54 col. 8, lines 6-10 col. 6, lines 28-33	2-8,10-19

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 JANUARY 1999	Date of mailing of the international search report 08 MAR 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PAUL E. CALLAHAN Telephone No. (703) 305-1336

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/15552

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EPO 0 680 187 A2 (GOVER ET AL) 02 November 1995, see entire document	1-19
X	EPO 0 420 779 A2 (DAWSON et al) 03 April 1991 col. 5, lines 15-23 col. 4, lines 14-18 col. 6, lines 2-8 col. 8, lines 2-8	2-8,9,10-19
Y	US 5,606,668 A (SHWED) 25 February 1997 col. 2, all col. 5, all col. 4, all	2-8, 10-19
X	US 5,835,726 A (SHWED et al.) 10 November 1998 col. 2, all col. 3, all AB	1-19
Y	US 5,577,202 A (PADGETT) 19 November 1996 col. 4, all	2-8,11-19
X	US 5,632,011 A (LANDFIELD et al.) 20 May 1997 Fig. 2A, 2B col. 4, all col. 2, all	1-8,9,10-19
Y	US 5,802,253 A (GROSS et al.) 01 September 1998 col. 1, all	2-8
A	US 5,555,346 A (GROSS et al.) 10 September 1996, see entire document	1-19
A	US 5,283,856 A (GROSS et al.) 01 February 1994, see entire document	1-19
A	US 5,331,543 A (YAJIMA et al.) 19 July 1994, see entire document	1-19
A	US 5,369,707 A (FOLLENDORE, III) 29 November 1994, see entire document	1-19
A	US 5,530,758 A (MARINO, Jr. et al.) 25 June 1996, see entire document	1-19

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/15532

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,414,833 A (HERSHEY et al.) 09 May 1995, see entire document	1-19
A	US 5,778,174 A (CAIN) 07 July 1998, see entire document	1-19
A	US 5,828,893 A (WIED et al.) 27 October 1998, see entire document	1-19
A	US 5,278,984 A (BATCHELOR) 11 January 1994, see entire document	1-19

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	ﾃｰﾏｺｰﾄﾞ(参考)
H04L 12/58		H04L 11/26	
12/22			

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

Fターム(参考) 5B089 GA31 HA10 HB07 JA31 KA17
KB13 KC52 KH30 LA00
5J104 AA01 JA13 NA02 PA08
5K030 GA15 HA05 HC01 LD19 MB18